Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. to 7. (cancelled)

[[9]] 8. (currently amended) A method of performing a transaction in a communication system between a first and a second participant wherein said second participant permits a service to be provided to said first participant in exchange for a payment, said method comprising the steps of:

a) upon initiation of said transaction by said first participant, said second participant sending a first message to said first participant, said first message including information pertaining to said second participant;

b) said first participant verifying said information pertaining to said second participant ~~to obtain assurance that said service will be provided upon assuring said payment~~;

c) said first participant generating a first value and a second value;

[[c)]] d) said first participant preparing a second message comprising said first value;

e) said first participant preparing a digital signature using said second message;

f) said first participant sending ~~a second message~~ said digital signature and information pertaining to said first participant to said second participant~~, said second message including information pertaining to said first participant~~;

[[d)]] g) said second participant verifying said information pertaining to said first participant ~~to obtain assurance that payment will be secured upon provision of said service~~; [[and]]

h) said second participant obtaining said second message using said digital signature and obtaining said first value using said second message;

i) said second participant sending said first value to said first participant to acknowledge provision of said service; and

j) said first participant verifying said first value and sending said second value to said second participant to enable said second participant to obtain said payment from a third participant using said second value.

~~e) upon verification of said information pertaining to said first participant, said second participant obtaining a digital signature for said first participant on said transaction using said second message, whereby said second participant may obtain said payment from a third~~

~~participant using said digital signature.~~

[[10]] 9. (currently amended) A method according to claim [[9]] 8 wherein said first participant is a holder of a card which performs cryptographic operations.

[[11]] 10. (currently amended) A method according to claim [[10]] 9 wherein said second participant is a terminal.

[[12]] 11. (currently amended) A method according to claim [[11]] 10 wherein said third participant is a financial institution.

[[13]] 12. (currently amended) A method according to claim [[9]] 8 wherein said information pertaining to said second participant included in said first message includes details and credentials of said second participant; and said first participant verifies said details and said credentials in step b).

[[14]] 13. (currently amended) A method according to claim [[9]] 8 wherein said information pertaining to said first participant included in said second message includes details and credentials of said first participant; and said second participant verifies said details and credentials in step [[d)]] g).

[[15]] 14. (currently amended) A method according to claim [[9]] 8 wherein said second message includes a challenge and step [[e)]] i) further comprises:

i) said second participant generating a response to said challenge;

ii) said second participant sending a third message including said response to said first participant;

iii) said first participant verifying said response; and

iv) said first participant sending a fourth message to said second participant such that said digital signature is provided by said second message and said fourth message.

[[16]] 15. (currently amended) A method according to claim [[15]] 14 further comprising:

i) said second participant verifying information in said fourth message;

ii) said second participant completing said transaction by providing said service; and

iii) said second participant sending said third participant a subset of said first, second, third and fourth messages to obtain said payment.

[[17]] 16. (currently amended) A method according to claim [[16]] 15 further comprising:

i) said third participant verifying said subset;

ii) said third participant providing said payment to said second participant.

[[18]] 17. (currently amended) A method according to claim [[13]] 12 wherein said credentials include a public key certificate.

[[19]] 18. (currently amended) A method according to claim [[15]] 14 wherein said challenge is a nonce.

19. (new) A system for performing a transaction between a first and second participant wherein said second participant permits a service to be provided to said first participant in exchange for a payment, said system comprising at least said second correspondent having a cryptographic processor that is configured for:

a) upon initiation of said transaction by said first participant, sending a first message to said first participant, said first message including information pertaining to said second participant;

b) receiving from said first participant, a digital signature and information pertaining to said first participant, said digital signature being prepared using a second message, said second message being prepared to comprise a first value, said first value being generated by said first participant along with a second value;

c) verifying said information pertaining to said first participant;

d) obtaining said second message using said digital signature and obtaining said first value using said second message;

e) sending said first value to said first participant to acknowledge provision of said service; and

f) receiving from said first participant, said second value upon said first participant verifying said first value, said second to be used to obtain payment from a third participant.

20. (new) The system according to claim 19 wherein said second participant is a terminal and

said first participant is a card which performs cryptographic operations.

21. (new) The system according to claim 20 wherein said third participant is a financial institution.

22. (new) The system according to claim 19 wherein said information pertaining to said second participant included in said first message includes details and credentials of said second participant.

23. (new) The system according to claim 19 wherein said information pertaining to said first participant included in said second message includes details and credentials of said first participant; and said second participant verifies said details and credentials in step c).

24. (new) The system according to claim 19 wherein said second message includes a challenge and step f) further comprises:

i) said second participant generating a response to said challenge;

ii) said second participant sending a third message including said response to said first participant; and

iii) said second participant receiving from said first participant upon said first participant verifying said response, a fourth message such that said digital signature is provided by said second message and said fourth message.

25. (new) The system according to claim 24 further comprising:

i) said second participant verifying information in said fourth message;

ii) said second participant completing said transaction by providing said service; and

iii) said second participant sending said third participant a subset of said first, second, third and fourth messages to obtain said payment.

26. (new) The system according to claim 25 further comprising:

i) said second participant obtaining said payment from said third participant upon said third participant verifying said subset.

27. (new) The system according to claim 22 wherein said credentials include a public key

certificate.

28. (new) The system according to claim 24 wherein said challenge is a nonce.